JUSTIFICATION
FOR AN EXCEPTION TO FAIR OPPORTUNITY

1. Contracting Activity: Department of Veterans Affairs (VA)
Office of Acquisition Operations
Technology Acquisition Center
23 Christopher Way
Eatontown, NJ 07724

2. Description of Action: This proposed action is for a Firm-Fixed-Price (FFP) Task Order (TO) is to procure two brand name FireEye physical appliances inclusive of warranty maintenance and software licenses for the VA Office of Information Technology Service Delivery and Enginerring Enterprise Operations (EO) Security Division. The solicitation will be issued under the National Aeronautics and Space Administration (NASA) Solutions for Enterprise-Wide Procurement (SEWP) IV Government-Wide Acquisition Contract (GWAC). The period of performance for this order shall be 12 months from receipt of order.

3. Description of the Supplies or Services: The proposed action is to procure a brand name FireEyee Analysis Execution (AX )5400 appliance and Forensics Platform (PX) 4 Gigabytes per Second (Gbps) Packet Capture appliance. As part of the procurement of these items, a 12-month warranty and maintenance period for the FireEye appliances and perpetual software licenses is included. The required warranty and maintenance includes 24/7 telephone and email support, software updates, patches and defect support for one year.

4. Statutory Authority: The statutory authority permitting an exception to fair opportunity is Section 41 U.S.C. 4106(c)(2) as implemented by the Federal Acquisition Regulation (FAR) Subpart 16.505(b)(2)(i)(B), entitled “Only one awardee is capable of providing the supplies or services required at the level of quality required because the supplies or services ordered are unique or highly specialized”.

5. Rationale Supporting Use of Authority Cited Above: This is a brand name justification in support of FAR 11.105, Items Peculiar to One Manufacturer. Based on extensive market research, as described in paragraph 8 of this document, it was determined that limited competition is available for the aforementioned brand name items and services.

VA’s Continuous Readiness Information Security Program requires system security monitoring of all system logs and network connectivity to provide event and log correlation, event alerting and information security threat intelligence, and reporting of all malware activity. VA utilizes a Security Information and Event Management (SIEM) for data center systems and networks. Using combined SIEM Malware plug-in data feeds from FireEye products, collectively referred to as FireEye brand name malware appliance and software meet these requirements. The malware protection appliance includes standard software and licenses.

Additionally, these malware protection appliances are provide functional requirements in support of VA's Information Technology visibility to the Network Initiative. Specifically, only FireEye brand name security appliances can provide upstream forwarding of any localized malware activity data into the existing EO FireEye architecture. The upstream of data is critical to produce a single view collective status of all security related activity over the network. This will ultimately provide EO a single interactive view that displays the monitored EO's network's security posture of all network elements of malware protection. No other brand name software cannot accomplish this due to the fact that another brand product cannot communicate, nor integrate with the architecture and software for the Enterprise Operations Console. This introduce risk to the Government in that it will not allow security visibility of malware activity on the network. Additionally, data monitored and provided by another vendor will not integrate with the existing toolset, which is based on FireEye brand name security architecture and licensing.

Included with the procurement of the appliances is FireEye brand name software. This required software is the only product that can integrate with the currently fielded VA architecture and FireEye-based malware protection licensing. Specifically, the current system and software communicates through source code that is based on FireEye proprietary data. This software allows the different hardware sensors and devices to interoperate with the central management console. No other software can provide this communication capability.

Failure to procure the required appliances with warranty maintenance and software will result in leaving VA possibly vulnerable to cyber attacks. Furthermore, there would be delayed incident response and possibly missing threat understanding against cyber attacks , such as Advanced Persistent Threat, Zero Day and Command and Control Information Technology Threats. This ends up harming VA's security posture to protect data center data, networks, and systems,and ultimately the Veteran.

6. Efforts to Obtain Competition: Market research was conducted, details of which are in the market research section of this document. This effort did not yield any additional sources that can meet the Government's requirements. It was determined however that limited competition is viable among authorized resellers for this brand name item. In accordance with FAR 5.301 and 16.505(b)(2), this action will be synopsized at award on the Federal Business Opportunities Page (FBO) and the justification will be made publicly available.

7. Actions to Increase Competition: In order to remove or overcome barriers to competition in future acquisitions for this requirement, the agency will work with the program office to continue to perform market research to consider and ascertain if any other sources can provide these services in the future.

8. Market Research: The Government's technical experts conducted market research in October 2014. Market research was completed by reviewing other similar malware protection full packet capture systems. The other similar software reviewed included International Business Machines (IBM) QRadar Packet Capture appliance, Solera Networks, and RSA NetWitness Decoder. Based on reviews of these products, the

Government's technical experts determined that none of the products can meet the Government's interoperability and compatibility requirements, nor the upstream forwarding requirment discussed above. Additionally, VA EO IT Security Subject Matter Experts regularly review industry trade publications and conduct internet research to ascertain if any other brand name software is available. Based on all of these market research efforts, the Government's technical experts have determined that only FireEye brand name security appliance and licensing can meet all of EO's needs

Additional market research was conducted in November 2014, utilizing the NASA SEWP IV GWAC Manufacturer lookup tool. Based on this research, there are multiple resellers that can provide the required licenses, therefore there is an expectation for limited competition at the reseller level.

9. Other Facts: N/A